MUTUAL AUTHENTICATION SYSTEM, MUTUAL AUTHENTICATION METHOD, MUTUAL AUTHENTICATION EQUIPMENT AND STORAGE MEDIUM

Publication number: JP2003124927 (A)

Publication date: 2003-04-25

Inventor(s): ISHIGURO RYUJI; TADA KEIKO + (ISHIGURO RYUJI, ; TADA KEIKO)

Applicant(s): SONY CORP + (SONY CORP)

Classification:

- international: G06F15/00; G06F21/20; G06Q10/00; G06Q30/00; G06Q50/00; H04L9/32; G06F15/00; G06F21/20; G06Q10/00; G06Q30/00; G06Q50/00; H04L9/32; (IPC1-7): G06F15/00; G06F17/60; H04L9/32

- European:

Application number: JP20010317328 20011015

Priority number(s): JP20010317328 20011015

Abstract of JP 2003124927 (A)

Translate this text

PROBLEM TO BE SOLVED: To perform mutual authentication by using NTRU public key encryption method. SOLUTION: Mutual authentication between a server and a client is performed with the protocol using an NTRU private key encryption method. By adding random numbers which are going to be seeds of a session key and their hash value to transmission data, it makes possible to check whether description failure is generated. The session key is formed on the basis of the random numbers for the session key, and data transmission and reception after authentication are performed by encryption. Process of the NTRU encryption method is light and the protocol is simple, so that mounting to an assembly type apparatus is enabled.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－124927
（P2003－124927A）
(43)公開日　平成15年４月25日(2003.4.25)

(51)Int.Cl.⁷	識別記号	Ｆ１	テーマコード（参考）
Ｈ０４Ｌ　9/32		Ｇ０６Ｆ　15/00	３３０Ｃ　５Ｂ０８５
Ｇ０６Ｆ　15/00	３３０	17/60	３０２Ｅ　５Ｊ１０４
17/60	３０２		３３２
	３３２		５１２
	５１２		ＺＥＣ

審査請求　未請求　請求項の数20　ＯＬ　（全 15 頁）　最終頁に続く

(21)出願番号　特願2001－317328(P2001－317328)

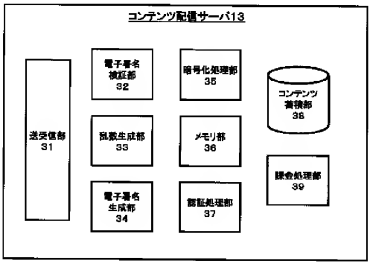
(22)出願日　平成13年10月15日(2001.10.15)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　石黒　隆二
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　多田　恵了
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100101801
弁理士　山田　英治　（外２名）

最終頁に続く

(54)【発明の名称】　相互認証システム及び相互認証方法、相互認証装置、並びに記憶媒体

(57)【要約】
【課題】　ＮＴＲＵ公開鍵暗号方式を使用して相互認証を行う。
【解決手段】　ＮＴＲＵ公開鍵暗号方式を用いたプロトコルによりサーバとクライアント間の相互認証を行う。また、送信データ中にセッション・キーの種となる乱数とそのハッシュ値を加えることにより、Ｄｅｃｒｉｐｔｉｏｎ　Ｆａｉｌｕｒｅが起きているかどうかをチェックできるようするとともに、セッション・キー用の乱数を基にセッション・キーを作り出して、認証後のデータ送受信を暗号化して行う。ＮＴＲＵの暗号化方式は処理が軽く簡単なプロトコルであることから、組み込み型機器に実装することが可能である。



1

【特許請求の範囲】

【請求項１】通信媒体を介して接続される複数の装置間で所定の公開鍵暗号方式を用いて相互認証を行う相互認証システムであって、

通信相手が互いにセッション・キーの種となる乱数を生成するセッション・キーの種生成手段と、

相互認証用のデータ中にセッション・キーの種となる乱数とそのハッシュ値を付加することによって、復号化の失敗が起きているかどうかをチェックする復号化検査手段と、を備えることを特徴とする相互認証システム。

【請求項２】前記公開鍵暗号方式は、ＮＴＲＵ公開鍵暗号方式である、ことを特徴とする請求項１に記載の相互認証システム。

【請求項３】前記復号化検査手段は、通信相手の公開鍵でセッション・キーの種となる乱数とそのハッシュ値を暗号化して送信するとともに、通信相手から受信したデータを自分の秘密鍵で復号化して、セッション・キーの種となる乱数とそのハッシュ値を取り出し、セッション・キーの種となる乱数のハッシュ値を算出してこれを取り出された該ハッシュ値と比較することによって、公開鍵における復号化に失敗したか否かを判別する、ことを特徴とする請求項１に記載の相互認証システム。

【請求項４】通信相手が互いに生成したセッション・キーの種を基にセッション・キーを生成するセッション・キー生成手段と、

該セッション・キーを用いた暗号データの送受信を行う暗号データ送受信手段と、

をさらに備えることを特徴とする請求項１に記載の相互認証システム。

【請求項５】通信媒体を介して接続される複数の装置間で所定の公開鍵暗号方式を用いて相互認証を行う相互認証方法であって、

通信相手が互いにセッション・キーの種となる乱数を生成するセッション・キーの種生成ステップと、

相互認証用のデータ中にセッション・キーの種となる乱数とそのハッシュ値を付加することによって、復号化の失敗が起きているかどうかをチェックする復号化検査ステップと、を備えることを特徴とする相互認証方法。

【請求項６】前記公開鍵暗号方式は、ＮＴＲＵ公開鍵暗号方式である、ことを特徴とする請求項５に記載の相互認証方法。

【請求項７】前記復号化検査ステップでは、通信相手の公開鍵でセッション・キーの種となる乱数とそのハッシュ値を暗号化して送信するとともに、通信相手から受信したデータを自分の秘密鍵で復号化して、セッション・キーの種となる乱数とそのハッシュ値を取り出し、セッション・キーの種となる乱数のハッシュ値を算出してこれを取り出された該ハッシュ値と比較することによって、公開鍵における復号化に失敗したか否かを判別する、ことを特徴とする請求項５に記載の相互認証方法。

2

【請求項８】通信相手が互いに生成したセッション・キーの種を基にセッション・キーを生成するステップと、

該セッション・キーを用いた暗号データの送受信を行うステップと、をさらに備えることを特徴とする請求項５に記載の相互認証方法。

【請求項９】第１の装置と第２の装置の間で所定の公開鍵暗号方式を用いて相互認証を行う相互認証方法であって、

第１の装置が自分の公開鍵E_aを含んだ電子署名C_aを第２の装置に送信するステップと、

第２の装置が、第１の装置の電子署名C_aを確認した後、相互認証用の乱数N_b及びセッション・キーの種S_bを生成するとともにS_bのハッシュ値Ｈａｓｈ（S_b）を計算して、N_b、S_b、Ｈａｓｈ（S_b）を第１の装置の公開鍵E_aで暗号化したデータE_a（N_b，S_b，Ｈａｓｈ（S_b））を、自分の公開鍵E_bを含んだ電子署名C_bとともに第１の装置に送信するステップと、

第１の装置が、第２の装置の電子署名C_bを確認した後、自分の秘密鍵で受信データE_a（N_b，S_b，Ｈａｓｈ（S_b））を復号化して、セッション・キーの種S_bのハッシュ値Ｈａｓｈ’（S_b）を計算して、受信したハッシュ値Ｈａｓｈ（S_b）と一致するか否かによって、公開鍵における復号化に失敗したか否かを判別するステップと、

復号化に失敗していないことに応答して、第１の装置が、相互認証用の乱数N_a及びセッション・キーの種S_aを生成するとともにS_aのハッシュ値Ｈａｓｈ（S_a）を計算して、N_a、S_a、Ｈａｓｈ（S_a）を第２の装置の公開鍵E_bで暗号化したデータE_b（N_a，S_a，Ｈａｓｈ（S_a））を、受信データから取り出した乱数N_bとともに第２の装置に送信するステップと、

第２の装置が、受信した乱数N_bが自分で生成した乱数と等しいか否かで第１の装置を本人確認するステップと、

本人確認に成功したことに応答して、第２の装置が、自分の秘密鍵で受信データE_b（N_a，S_a，Ｈａｓｈ（S_a））を復号化して、セッション・キーの種S_aのハッシュ値Ｈａｓｈ’（S_a）を計算して、受信したハッシュ値Ｈａｓｈ（S_a）と一致するか否かによって、公開鍵における復号化に失敗したか否かを判別するステップと、

復号化に失敗していないことに応答して、第２の装置が、相互認証用の乱数N_aを第１の装置に送信するステップと、

第１の装置が、受信した乱数N_aが自分で生成した乱数と等しいか否かで第２の装置を本人確認するステップと、を具備することを特徴とする相互認証方法。

【請求項１０】前記公開鍵暗号方式は、ＮＴＲＵ公開鍵暗号方式である、ことを特徴とする請求項９に記載の相互認証装置。

【請求項１１】第１及び第２の装置がそれぞれ互いに生成したセッション・キーの種S_a及びS_bを基にセッション・キーを生成するステップと、
第１及び第２の装置が該セッション・キーを用いた暗号データの送受信を行うステップと、をさらに備えることを特徴とする請求項９に記載の相互認証方法。
【請求項１２】通信媒体を介して接続される他の装置との間で所定の公開鍵暗号方式を用いて相互認証を行う相互認証装置であって、
相互認証用の乱数Ｎを発生する手段と、
セッション・キーの種となる乱数Ｓを発生する手段と、
セッション・キーの種のハッシュ値Ｈを計算する手段と、
乱数Ｎとセッション・キーの種Ｓとセッション・キーの種のハッシュ値Ｈを通信相手の公開鍵で暗号化して送信する手段と、
通信相手から受信した暗号データを自分の公開鍵で復号化して、通信相手の相互認証用の乱数Ｎ'と通信相手が生成したセッション・キーの種Ｓ'及びそのハッシュ値Ｈ'を取り出す手段と、
セッション・キーの種Ｓ'のハッシュ値Ｈ"を計算して、Ｈ'とＨ"が一致するか否かによって公開鍵における復号化に失敗したか否かを検査する手段と、をを具備することを特徴とする相互認証装置。
【請求項１３】前記公開鍵暗号方式は、ＮＴＲＵ公開鍵暗号方式である、ことを特徴とする請求項１２に記載の相互認証装置。
【請求項１４】通信相手から受信した暗号データから取り出した通信相手の相互認証用の乱数Ｎ'を通信相手に送信する手段と、
通信相手から受信した自分の相互認証用の乱数が、自分で発生した乱数Ｎと等しいか否かで、通信相手を本人確認する手段と、をさらに備えることを特徴とする請求項１２に記載の相互認証装置。
【請求項１５】自身で生成したセッションキーの種Ｓ及び他の装置から受信したセッションキーの種Ｓ' を基にセッション・キーを生成する手段と、
該セッション・キーを用いて他の装置との暗号データの送受信を行う手段と、をさらに備えることを特徴とする請求項１２に記載の相互認証装置。
【請求項１６】他の装置との間で所定の公開鍵暗号方式を用いて相互認証を行う相互認証方法であって、
相互認証用の乱数Ｎを発生するステップと、
セッション・キーの種となる乱数Ｓを発生するステップと、
セッション・キーの種のハッシュ値Ｈを計算するステップと、
乱数Ｎとセッション・キーの種Ｓとセッション・キーの種のハッシュ値Ｈを通信相手の公開鍵で暗号化して送信するステップと、
通信相手から受信した暗号データを自分の公開鍵で復号化して、通信相手の相互認証用の乱数Ｎ'と通信相手が生成したセッション・キーの種Ｓ'及びそのハッシュ値Ｈ'を取り出すステップと、
セッション・キーの種Ｓ'のハッシュ値Ｈ"を計算して、Ｈ'とＨ"が一致するか否かによって公開鍵における復号化に失敗したか否かを検査するステップと、を具備することを特徴とする相互認証方法。
【請求項１７】前記公開鍵暗号方式は、ＮＴＲＵ公開鍵暗号方式である、ことを特徴とする請求項１６に記載の相互認証方法。
【請求項１８】通信相手から受信した暗号データから取り出した通信相手の相互認証用の乱数Ｎ'を通信相手に送信するステップと、
通信相手から受信した自分の相互認証用の乱数が、自分で発生した乱数Ｎと等しいか否かで、通信相手を本人確認するステップと、をさらに備えることを特徴とする請求項１６に記載の相互認証方法。
【請求項１９】自身で生成したセッションキーの種Ｓ及び他の装置から受信したセッションキーの種Ｓ' を基にセッション・キーを生成するステップと、
該セッション・キーを用いて他の装置との暗号データの送受信を行うステップと、をさらに備えることを特徴とする請求項１６に記載の相互認証方法。
【請求項２０】他の装置との間で所定の公開鍵暗号方式を用いて相互認証を行うための相互認証処理をコンピュータ・システム上で実行するように記述されたコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータ・ソフトウェアは、
相互認証用の乱数Ｎを発生するステップと、
セッション・キーの種となる乱数Ｓを発生するステップと、
セッション・キーの種のハッシュ値Ｈを計算するステップと、
乱数Ｎとセッション・キーの種Ｓとセッション・キーの種のハッシュ値Ｈを通信相手の公開鍵で暗号化して送信するステップと、
通信相手から受信した暗号データを自分の公開鍵で復号化して、通信相手の相互認証用の乱数Ｎ'と通信相手が生成したセッション・キーの種Ｓ'及びそのハッシュ値Ｈ'を取り出すステップと、
セッション・キーの種Ｓ'のハッシュ値Ｈ"を計算して、Ｈ'とＨ"が一致するか否かによって公開鍵における復号化に失敗したか否かを検査するステップと、を具備することを特徴とする記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、２以上の機器間で相互認証システム及び相互認証方法、相互認証装置、並

びに記憶媒体に係り、特に、音楽や画像などの有料コンテンツの配信において課金処理時に相互認証を行う相互認証システム及び相互認証方法、相互認証装置、並びに記憶媒体に関する。

【０００２】更に詳しくは、本発明は、公開鍵暗号方式を用いて相互認証を行う相互認証システム及び相互認証方法、相互認証装置、並びに記憶媒体に係り、特に、比較的処理が軽い公開鍵暗号方式を用いて携帯端末のような組み込み機器上でも相互認証を行うことができる相互認証システム及び相互認証方法、相互認証装置、並びに記憶媒体に関する。

【０００３】

【従来の技術】昨今、情報通信技術の飛躍的な進歩とも相俟って、コンピュータを始めとする各種の情報機器が電話回線やインターネットなどの広域ネットワークに接続され、コンピュータ資源の共有や、情報の共有・流通・配布・交換などの協働的作業を円滑に行うことができるようになってきている。

【０００４】ネットワークは、単なる情報配信の手段としてだけではなく、音楽や画像などの有料コンテンツの販売や、従来の物流に置き換わる「ネット販売」や「オンライン・ショッピング」にも活用されている。また、コンテンツや商品の購入手続だけではなく、電子マネーなどを利用して課金処理もネットワーク上で無人化・自動化することができる。

【０００５】例えば、ＰＤＡ（Personal Digital Assistant）のような携帯情報端末に携帯電話機を接続することにより、電話網やインターネット網を介してコンテンツをダウンロードすることによって、ＰＤＡ上でコンテンツを再生して楽しむということができる。

【０００６】他方、デジタル形式のデータやコンテンツの複製や改竄は極めて容易であり、著作権侵害の危険に無防備にさらされているとさえ言える。したがって、著作権法やその他の複製に関する法規制を強化するだけでは不充分であり、情報技術の観点からもデータやコンテンツの保護を拡充する必要があると思料される。

【０００７】また、従来の物流とは相違し、ネットワーク取引においては、顔が見えない相手にコンテンツを渡したり対価を支払ったりしなければならず、コンテンツを無断複製や改竄などの海賊行為から保護したり、ユーザのプライバシをなりすましによる侵害から充分に保護することが充分にできない可能性がある。

【０００８】このため、ネットワーク世界では、正当な相手とのみ取引を行うべく、「相互認証」という手続が広く採り入れられている。

【０００９】相互認証には、いわゆる「公開鍵暗号方式」を適用することが一般的である。ここで、公開鍵暗号とは、データを暗号化する際に用いる鍵と、復号化する際に用いる鍵が異なり、「非対称暗号」とも呼ばれる。公開鍵暗号アルゴリズムは、一方の鍵から他方の鍵を算出することが非常に困難であるという性質を持つことにより、一方の鍵で暗号化した情報は他方の鍵でしか復号化できないことが保証される。暗号化の鍵は「公開鍵」と呼ばれ、一般に公開して誰でも使用できるようにする。また、復号化の鍵は「秘密鍵」と呼ばれ、他人に漏れないように所有者が管理する。

【００１０】公開鍵暗号方式を採用した場合、各自は復号鍵として自分の秘密鍵を１つ所有するだけでよいので、システム全体で使用する鍵の数を少なくすることができ、管理が容易になる。

【００１１】しかしながら、公開鍵暗号方式は、一般に、暗号化並びに復号化の処理が重たく、ＣＰＵパワーやメモリ容量を要する。量的にかなり小さい情報であれば、暗号化・復号化には実用上の支障はないが、音楽や画像などの比較的大きな情報の場合には支障が生じる。また、ＰＤＡのような小型（すなわちＣＰＵパワーが非力）でバッテリ駆動の組み込み機器の場合には、相互認証に公開鍵暗号方式を用いるのは困難である。

【００１２】しかしながら、もし、セッション・キー発生に使用される乱数などのデータが平文のまま通信路を流れると、通信路のデータが見られた場合には、それらの乱数を使って悪者がセッション・キーを簡単に作り出して、さまざまな不正を働く危険がある。

【００１３】このような問題を解消するために、”ＮＴＲＵ（エヌトゥルー）”と呼ばれる、短く且つ用意に鍵を生成し、高速且つ小メモリ容量で実現可能な公開鍵暗号方式が開発・提供されている。

【００１４】ＮＴＲＵは世界で最も速く安全な公開鍵暗号システムであり、その処理速度は従来の公開鍵暗号システムと比べて２０倍から４００倍にも達する。また、ＮＴＲＵは、システムの拡張が容易であり、頻繁なワイヤレス取引や音楽やゲームをダウンロードするために接続される数十億の消費者向けデバイスを保護するインフラストラクチャーの構築も可能である。一方、ＮＴＲＵは低価格で大量に販売されるデバイスのセキュリティを、小さな構成で確実かつ効率的に守ることもできる。さらにＮＴＲＵは、新規のセキュリティ・パラダイムを使用して、付加価値の高いコミュニケーションとコンテンツのセキュリティを厳重に保護することもできる（http://www.ntru.co.jp/）。

【００１５】ＮＴＲＵは、因数分解や対数問題を使用しない、初の安全で実用的な公開鍵暗号システムである。ＮＴＲＵのアルゴリズムを実行する計算プロセスは単純であるので、低価格の８ビット・マイクロプロセッサでも高速に処理することができる。すなわち、ＮＴＲＵの公開鍵暗号方式は、比較的軽い処理で且つ小メモリ容量で実現できることから、携帯電話機、デジタル・ミュージック・プレーヤや、ＰＤＡなどのデバイスの使用時に、プライバシーと信頼性を確立することができると思料される。

【００１６】しかしながら、ＮＴＲＵは処理が軽い反面、復号化（Ｄｅｃｒｙｐｔ）の際に基データが異なるというエラー（Ｄｅｃｒｙｐｔｉｏｎ　Ｆａｉｌｕｒｅ）を発生することがある。

【００１７】Ｄｅｃｒｙｐｔｉｏｎ　Ｆａｉｌｕｒｅが起こると、端末間で再度セッション確立などの手続を繰り返さなければならず、それまでに行われた相互認証などの処理がすべて無駄になってしまう。例えば、携帯電話などの機器からサーバに再接続しなければならず、処理時間だけでなく通信費も無駄になってしまう。

【００１８】

【発明が解決しようとする課題】本発明の目的は、音楽や画像などの有料コンテンツの配信において課金処理時に相互認証を好適に行うことができる、優れた相互認証システム及び相互認証方法、相互認証装置、並びに記憶媒体を提供することにある。

【００１９】本発明の更なる目的は、公開鍵暗号方式を用いて機器間の相互認証を好適に行うことができる、優れた相互認証システム及び相互認証方法、相互認証装置、並びに記憶媒体を提供することにある。

【００２０】本発明の更なる目的は、比較的処理が軽い公開鍵暗号方式を用いて携帯端末のような組み込み機器上でも相互認証を行うことができる、優れた相互認証システム及び相互認証方法、相互認証装置、並びに記憶媒体を提供することにある。

【００２１】

【課題を解決するための手段及び作用】本発明は、上記課題を参酌してなされたものであり、その第１の側面は、通信媒体を介して接続される複数の装置間で所定の公開鍵暗号方式を用いて相互認証を行う相互認証システム又は相互認証方法であって、通信相手が互いにセッション・キーの種となる乱数を生成するセッション・キーの種生成手段又はステップと、相互認証用のデータ中にセッション・キーの種となる乱数とそのハッシュ値を付加することによって、復号化の失敗が起きているかどうかをチェックする復号化検査手段又はステップと、を備えることを特徴とする相互認証システム又は相互認証方法である。

【００２２】但し、ここで言う「システム」とは、複数の装置（又は特定の機能を実現する機能モジュール）が論理的に集合した物のことを言い、各装置や機能モジュールが単一の筐体内にあるか否かは特に問わない。

【００２３】本発明の第１の側面に係る相互認証システムは、ＣＰＵパワーが非力でメモリ容量が小さな携帯情報端末の相互認証を行うことを考慮して、ＮＴＲＵ公開鍵暗号方式を用いた相互認証処理を行う。

【００２４】ＮＴＵＲ公開鍵暗号方式を用いた場合、復号化の失敗（ＤｅｃｒｉｐｔｉｏｎＦａｉｌｕｒｅ）が発生する可能性がある。そこで、本発明の第１の側面に係る相互認証システムでは、通信相手が互いにセッション・キーの種となる乱数を生成するとともに、相互認証用のデータ中にセッション・キーの種となる乱数とそのハッシュ値を付加することによって、復号化の失敗が起きているかどうかをチェックするようにした。この結果、確かなセッション確立でセッション・キーを共有することができる。

【００２５】ここで、前記復号化検査手段又はステップは、通信相手の公開鍵でセッション・キーの種となる乱数とそのハッシュ値を暗号化して送信するとともに、通信相手から受信したデータを自分の秘密鍵で復号化して、セッション・キーの種となる乱数とそのハッシュ値を取り出し、セッション・キーの種となる乱数のハッシュ値を算出してこれを取り出された該ハッシュ値と比較することによって、公開鍵における復号化に失敗したか否かを判別することができる。

【００２６】また、復号化の失敗が起きていないと判断された場合には、通信相手が互いに生成したセッション・キーの種を基にセッション・キーを生成して、該セッション・キーを用いた暗号データの送受信を行うことができる。すなわち、課金処理やコンテンツの配信などの手続を、安全な通信路を介して行うことが可能となる。

【００２７】また、本発明の第２の側面は、第１の装置と第２の装置の間で所定の公開鍵暗号方式を用いて相互認証を行う相互認証方法であって、第１の装置が自分の公開鍵E_aを含んだ電子署名C_aを第２の装置に送信するステップと、第２の装置が、第１の装置の電子署名C_aを確認した後、相互認証用の乱数N_b及びセッション・キーの種S_bを生成するとともにSbのハッシュ値Ｈａｓｈ（S_b）を計算して、N_b、S_b、Ｈａｓｈ（S_b）を第１の装置の公開鍵E_aで暗号化したデータE_a（N_b，S_b，Ｈａｓｈ（S_b））を、自分の公開鍵E_bを含んだ電子署名C_bとともに第１の装置に送信するステップと、第１の装置が、第２の装置の電子署名C_bを確認した後、自分の秘密鍵で受信データE_b（N_b，S_b，Ｈａｓｈ（S_b））を復号化して、セッション・キーの種S_bのハッシュ値Ｈａｓｈ’（S_b）を計算して、受信したハッシュ値Ｈａｓｈ（S_b）と一致するか否かによって、公開鍵における復号化に失敗したか否かを判別するステップと、復号化に失敗していないことに応答して、第１の装置が、相互認証用の乱数N_a及びセッション・キーの種S_aを生成するとともにSaのハッシュ値Ｈａｓｈ（S_a）を計算して、N_a、S_a、Ｈａｓｈ（S_a）を第２の装置の公開鍵E_bで暗号化したデータE_b（N_a，S_a，Ｈａｓｈ（S_a））を、受信データから取り出した乱数N_bとともに第２の装置に送信するステップと、第２の装置が、受信した乱数N_bが自分で生成した乱数と等しいか否かで第１の装置を本人確認するステップと、本人確認に成功したことに応答して、第２の装置が、自分の秘密鍵で受信データE_b（N_a，S_a，Ｈａｓｈ（S_a））を復号化して、セッション・キーの種S_aのハッシュ値

Ｈａｓｈ’（Ｓａ）を計算して、受信したハッシュ値Ｈａｓｈ（Ｓａ）と一致するか否かによって、公開鍵における復号化に失敗したか否かを判別するステップと、復号化に失敗していないことに応答して、第２の装置が、相互認証用の乱数Naを第１の装置に送信するステップと、第１の装置が、受信した乱数Naが自分で生成した乱数と等しいか否かで第２の装置を本人確認するステップと、を具備することを特徴とする相互認証方法である。

【００２８】ここで、ＣＰＵパワーが非力でメモリ容量が小さな携帯情報端末の相互認証を行うことを考慮して、ＮＴＲＵ公開鍵暗号方式を用いた相互認証処理を行う。

【００２９】本発明の第２の側面に係る相互認証方法によれば、第１及び第２の装置は、通信相手を相互認証するとともに、お互いが正しく公開鍵で暗号化された乱数を復号化することができたか否かによって、復号化の失敗を起していないことを確認することができる。また、復号化の失敗を起していない場合のみ、互いに生成した種Ｓａ及びＳｂからセッション・キーを生成する。そして、その後のデータのやり取りを、セッション・キーで暗号化して送受信することにより、第３者による改竄や盗聴を防ぐことができる。

【００３０】また、本発明の第３の側面は、通信媒体を介して接続される他の装置との間で所定の公開鍵暗号方式を用いて相互認証を行う相互認証装置又は相互認証方法であって、相互認証用の乱数Ｎを発生する手段又はステップと、セッション・キーの種となる乱数Ｓを発生する手段又はステップと、セッション・キーの種のハッシュ値Ｈを計算する手段又はステップと、乱数Ｎとセッション・キーの種Ｓとセッション・キーの種のハッシュ値Ｈを通信相手の公開鍵で暗号化して送信する手段又はステップと、通信相手から受信した暗号データを自分の公開鍵で復号化して、通信相手の相互認証用の乱数Ｎ’と通信相手が生成したセッション・キーの種Ｓ’及びそのハッシュ値Ｈ’を取り出す手段又はステップと、セッション・キーの種Ｓ’のハッシュ値Ｈ”を計算して、Ｈ’とＨ”が一致するか否かによって公開鍵における復号化に失敗したか否かを検査する手段又はステップと、を具備することを特徴とする相互認証装置又は相互認証方法である。

【００３１】ここで、ＣＰＵパワーが非力でメモリ容量が小さな携帯情報端末の相互認証を行うことを考慮して、ＮＴＲＵ公開鍵暗号方式を用いた相互認証処理を行う。

【００３２】また、本発明の第３の側面に係る相互認証装置又は相互認証方法は、通信相手から受信した暗号データから取り出した通信相手の相互認証用の乱数Ｎ’を通信相手に送信する手段又はステップと、通信相手から受信した自分の相互認証用の乱数が、自分で発生した乱数Ｎと等しいか否かで、通信相手を本人確認する手段又はステップとをさらに備えていてもよい。

【００３３】本発明の第３の側面に係る相互認証装置又は相互認証方法によれば、第１及び第２の装置は、通信相手を相互認証するとともに、お互いが正しく公開鍵で暗号化された乱数を復号化することができたか否かによって、復号化の失敗を起していないことを確認することができる。また、復号化の失敗を起していない場合のみ、互いに生成した種Ｓａ及びＳｂからセッション・キーを生成する。そして、その後のデータのやり取りを、セッション・キーで暗号化して送受信することにより、第３者による改竄や盗聴を防ぐことができる。

【００３４】また、本発明の第４の側面は、他の装置との間で所定の公開鍵暗号方式を用いて相互認証を行うための相互認証処理をコンピュータ・システム上で実行するように記述されたコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納した記憶媒体であって、前記コンピュータ・ソフトウェアは、相互認証用の乱数Ｎを発生するステップと、セッション・キーの種となる乱数Ｓを発生するステップと、セッション・キーの種のハッシュ値Ｈを計算するステップと、乱数Ｎとセッション・キーの種Ｓとセッション・キーの種のハッシュ値Ｈを通信相手の公開鍵で暗号化して送信するステップと、通信相手から受信した暗号データを自分の公開鍵で復号化して、通信相手の相互認証用の乱数Ｎ’と通信相手が生成したセッション・キーの種Ｓ’及びそのハッシュ値Ｈ’を取り出すステップと、セッション・キーの種Ｓ’のハッシュ値Ｈ”を計算して、Ｈ’とＨ”が一致するか否かによって公開鍵における復号化に失敗したか否かを検査するステップと、を具備することを特徴とする記憶媒体である。

【００３５】本発明の第４の側面に係る記憶媒体は、例えば、さまざまなプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・ソフトウェアをコンピュータ可読な形式で提供する媒体である。このような媒体は、例えば、ＣＤ（Compact Disc）やＦＤ（Floppy Disk）、ＭＯ（Magneto-Optical disc）などの着脱自在で可搬性の記憶媒体である。あるいは、ネットワーク（ネットワークは無線、有線の区別を問わない）などの伝送媒体などを経由してコンピュータ・ソフトウェアを特定のコンピュータ・システムに提供することも技術的に可能である。

【００３６】このような記憶媒体は、コンピュータ・システム上で所定のコンピュータ・ソフトウェアの機能を実現するための、コンピュータ・ソフトウェアと記憶媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、本発明の第４の側面に係る記憶媒体を介して所定のコンピュータ・ソフトウェアをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発

明の第３の側面に係る相互認証装置又は相互認証方法と同様の作用効果を得ることができる。

【００３７】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００３８】

【発明の実施の形態】本発明は、ＮＴＲＵ　Ｃｒｙｐｔｏｓｙｓｔｅｍｓ社が発案した公開鍵暗号方式を使用した相互認証プロトコルを提案するものである。

【００３９】ＮＴＲＵは、因数分解や対数問題を使用しない、初の安全で実用的な公開鍵暗号システムである。ＮＴＲＵのアルゴリズムを実行する計算プロセスは単純であり、低価格の８ビット・マイクロプロセッサでも高速に処理することができる。すなわち、ＮＴＲＵの公開鍵暗号方式は、比較的軽い処理で且つ小メモリ容量で実現できることから、サーバとクライアント間、とりわけ、携帯電話機、デジタル・ミュージック・プレーヤや、ＰＤＡなどの携帯型のデバイスにおいて、例えば音楽などのコンテンツ配信サイトとの間での相互認証手続に適用することができる。

【００４０】Ａ．ＮＴＲＵ公開鍵暗号システム

ここで、ＮＴＲＵの公開鍵暗号システムについて説明しておく。

【００４１】ＮＴＲＵの暗号化処理は、多項式代数、並びに、ｐとｑ２個のレダクション・モジュロに基づく混合システムを用いる。一方、その復号化処理は、非混合システムを使用し、その有効性は基本的な確立理論に依存する。ＮＴＲＵの公開鍵暗号システムのセキュリティは、多項式混合システムとリダクション・モジュロｐ及びｑの独立性との相互作用によって導き出される。このセキュリティは、ほとんどの格子において、適度に短い場合とは反対に、極端に短いベクトルを探すことは極めて難しいという事実（実験的にも観察されている）にも依拠する。

【００４２】ＮＴＲＵ暗号化システムは、（Ｎ．ｐ，ｑ）という３つの整数パラメータと、整数係数を持つＮ－１等級の４組の多項式L_f，L_g，L_ϕ，L_mで成り立つ。ここで、ｐとｑは素数である必要はないがｇｃｄ（ｐ，ｑ）＝１（最大公約数が１）であることと、ｑは常にｐよりも相当大きな数であることを前提とする。ここで、ド式で表されるリングＲを導入する。

【００４３】

【数１】

$$R = Z[X]/(X^N - 1)$$

【００４４】要素Ｆ（∈Ｒ）は、以下に示すような多項式又はベクトルで表現される。

【００４５】

【数２】

$$F = \sum_{i=0}^{N-1} F_i x^i = [F_0, F_1, \cdots, F_{N-1}]$$

【００４６】また、リングＲの乗算は記号"＊"を丸囲みした演算子で表記される。この演算子は、巡回畳み込み積であり、例えばＦとＧの巡回畳み込み積はド式の通りとなる。

【００４７】

【数３】

$$F \otimes G = H$$

$$\text{但し、} H_k = \sum_{i=0}^{k} F_i G_{k-i} + \sum_{i=k+1}^{N-1} F_i G_{N+k-i} = \sum_{i+j=k(\bmod N)} F_i G_j$$

【００４８】ＮＴＲＵ鍵を生成するために、復号者側では２つの多項式ｆ，ｇ（∈L_g）を選択する。一方の多項式ｆは、モジュロｑとモジュロｐそれぞれの逆数を持つという付加的な要件を満足する。ここで、それぞれの※逆数をF_q及びF_pとおくと、これらは下式のように表される。

【００４９】

【数４】

$$F_q \otimes f = 1 (\bmod\ q) \quad and \quad F_p \otimes f = 1 (\bmod\ p) \qquad (1)$$

【００５０】復号者側では次いで以下の量を計算する。

【００５１】

【数５】

$$h = F_q \otimes g \ (\bmod\ p) \qquad (2)$$

【００５２】復号者側における公開鍵は上式で表される多項式ｈである。また、復号者側における秘密鍵は、多項式ｆである。但し、復号側では、F_fも併せて保管しておきたくなるのが実情である。

【００５３】他方、暗号者側が復号者側にメッセージを送信したい場合、まず、平文の組L_mの中からメッセージｍを選択する。次いで、１つの多項式φ（∈L_ϕ）をランダムに選択して、復号者側の公開鍵ｈを用いて以下の計算を行う。

【００５４】

【数６】

$$e = p\phi \otimes h \ (\bmod\ q)$$

【００５５】上式が暗号者側から復号者側に送信された

暗号化メッセージｅとなる。

【００５６】復号者側が、受信した暗号化メッセージｃを復号化したい場合には、自分の秘密鍵ｆを用いる（この復号化処理を効率的に行いたい場合にはF_pを用いればよい）。

【００５７】暗号化メッセージｅを復号化したい場合には、まず下式を計算する。

【００５８】

【数７】

$$a = f \otimes e \pmod{q}$$

【００５９】ここで、復号者はａの係数を－ｑ／２～ｑ／２の範囲内で選択する。式ａを整数係数を持つ多項式として取り扱うことにより、以下の式を計算することで元のメッセージを再現することができる。

【００６０】

【数８】

$$F_p \otimes a \pmod{p}$$

【００６１】以上説明してきたように、ＮＴＲＵ公開鍵暗号方式によれば、適切なパラメータ値を用いることにより、極めて高い確率で復号化処理により元のメッセージを再現することができる。しかしながら、パラメータの選択次第で、Ｄｅｃｒｙｐｔｉｏｎ　Ｆａｉｌｕｒｅを生じる可能性（すなわち、正確に復号化されないという可能性）がある。

【００６２】Ｂ．相互認証プロトコル

以下、図面を参照しながら、本発明の実施形態について詳解する。

【００６３】本発明に係る相互認証プロトコルは、例えばサーバとクライアント間、とりわけ、携帯電話機、デジタル・ミュージック・プレーヤや、ＰＤＡ（Personal Digital Assistant）などの携帯型のデバイスにおいて、例えば音楽などのコンテンツ配信サイトとの間での相互認証に適用することができる。

【００６４】図１には、携帯端末に対してコンテンツ配信サービスを提供するネットワーク・システムの構成を模式的に示している。

【００６５】同図に示すように、ネットワーク・システムは、インターネット１１のような広域的なネットワークと、携帯電話機などの移動体に対してパケット通信などのサービスを提供する移動体通信網１２と、その他の図示しないネットワークで構成される。移動体通信網１２やその他のネットワークは、インターネット１１に相互接続されている。

【００６６】インターネット１１上には、無数のサーバが存在する。このうちの一部は、音楽や画像などのコンテンツを有料で配信するコンテンツ配信サーバ１３である。コンテンツ配信サーバ１３は、アクセス・ポイントを介してインターネット接続されているパーソナル・コンピュータなどの情報端末や、携帯電話機１４を接続することで移動体通信網１２経由でインターネット１１にアクセスするＰＤＡなどの情報端末１５に対して、有料でコンテンツの配信サービスを行う。

【００６７】［従来の技術］の欄でも既に述べたように、ネットワーク世界では顔が見えない相手とコンテンツのの引渡しや対価の支払いなどの手続きを行なわなければならない。このため、コンテンツを無断複製や改竄などの海賊行為から保護したり、ユーザのプライバシのなりすましによる侵害から保護しなければならない。

【００６８】このため、本実施形態に係るネットワーク・システム上では、コンテンツ配信サーバ１３がパーソナル・コンピュータや情報端末１５に対してコンテンツ配信サービスを行う際に、相互認証手続を採り入れている。また、携帯情報端末１５の処理能力やメモリ能力を考慮して、処理が軽く且つ簡単なプロトコルで実装可能なＮＴＲＵ公開鍵暗号方式（前述）を用いた相互認証を採用している。

【００６９】図２には、本実施形態に係るネットワーク・システム上でのコンテンツ配信サービスの流れを概略的に示している。

【００７０】まず、コンテンツ配信サーバ１３は、取引相手となる携帯情報端末１５と接続してセッションが確立すると（ステップＳ１）、相互認証並びにセッション・キーの生成を行う（ステップＳ２）。

【００７１】次いで、コンテンツ配信サーバ１３は、携帯情報端末１５に対して課金処理を行う（ステップＳ３）。課金処理は、前ステップＳ２で生成されたセッション・キーを用いることで、安全な通信路を介して行うことができる。

【００７２】次いで、コンテンツ配信サーバ１３は、セッション・キーを用いてコンテンツ復号鍵を暗号化して、携帯情報端末１５に送信する（ステップＳ４）。そして、注文を受けたコンテンツを暗号化してから、携帯情報端末１５に送信する（ステップＳ５）。

【００７３】これに対し、携帯情報端末１５側では、受信したコンテンツ復号鍵をセッション・キーで復号化するとともに、このコンテンツ復号鍵を用いて受信した暗号化コンテンツを復号化する（ステップＳ６）。そして、コンテンツを再生して視聴して楽しむことができる。

【００７４】なお、図２に示したフローにおいて、課金処理とコンテンツの配信処理の順番を入れ替えてもよい。

【００７５】本実施形態では、ＣＰＵパワーが非力でメモリ容量が小さな携帯情報端末の相互認証を行うことを考慮して、ステップＳ２における相互認証処理にＮＴＲＵ公開鍵暗号方式を用いたプロトコルを使用する。後述するように、本実施形態に係る相互認証プロトコルでは、通信相手が互いに乱数生成したセッション・キー用

の種を基にセッション・キーを作り出して、認証後のデータ送受信を暗号化して行うようになっている。

【００７６】また、送信データ中にセッション・キーの種となる乱数とそのハッシュ値を加えることにより、Ｄｅｃｒｉｐｔｉｏｎ　Ｆａｉｌｕｒｅが起きているかどうかをチェックするようにした。この結果、Ｄｅｃｒｉｐｔｉｏｎ　Ｆａｉｌｕｒｅが起きているかどうかをチェックして、確かなセッション確立でセッション・キーを共有することができる。

【００７７】図３には、コンテンツ配信サーバ１３の機能構成を模式的に示している。同図に示すように、コンテンツ配信サーバ１３は、インターネット１１などのネットワーク経由でメッセージの送受信を行うための送受信部３１と、携帯情報端末１５などの外部の装置から受信した電子署名を検証する電子署名検証部３２と、乱数生成部３３と、サーバ１３自身の電子署名を生成する電子署名生成部３４と、送信メッセージの暗号化や受信メッセージの復号化を行う暗号処理部３５と、発生した乱数やサーバ１３自身の秘密鍵・公開鍵や通信相手の公開鍵など所定のデータを保存するメモリ部３６と、認証処理部３７と、配信コンテンツを蓄積するコンテンツ蓄積部３８と、コンテンツ配信サービスを受けた外部の装置に対して課金処理を行う課金処理部３９を備えている。

【００７８】電子署名検証部３２は、送受信部３１で受信された携帯情報端末１４の電子署名ＣｅｒｔｉｆｏｃａｔｉｏｎＡを検証するとともに、この電子署名に含まれる携帯情報端末１５の公開鍵E_aを取り出して、メモリ部３６に保存しておく。

【００７９】乱数発生部３３は、相互認証に用いられる乱数N_bを生成したり、セッション・キーの種となる乱数S_bを生成する。これらの乱数N_b及びS_bは、携帯情報端末１５などの通信相手とセッションが確立している間はメモリ部３６に保存されている。

【００８０】電子署名生成部３４は、コンテンツ配信サーバ１３自身の公開鍵E_bをメモリ部３６から取り出して、このE_bを含んだ電子署名ＣｅｒｔｉｆｉｃａｔｉｏｎＢを生成して、送受信部３１からコンテンツ配信先となる携帯情報端末１５に送信する。

【００８１】暗号処理部３５は、携帯情報端末１５などの通信相手に送信するデータを相手の公開鍵E_aで暗号化したり、逆に携帯情報端末１５から受信したデータを自分自分の秘密鍵で復号化したりする。また、暗号処理部３５は、通信相手と交換し合った互いのセッション・キーの種を基にセッション・キーを生成して、認証処理後の送信データの暗号化に用いることができる。

【００８２】認証処理部３７は、携帯情報端末１５などのコンテンツ配信先との間で認証処理を行う。例えば、通信相手からの受信メッセージに含まれるデータのハッシュ値を計算して、同じく受信メッセージに含まれるハッシュ値と照合することにより、通信相手が本物であるか否かを判別することができる。また、相互認証処理にＮＴＲＵ公開鍵暗号方式を用いているが、認証処理部３７は、ハッシュ値の照合により、Ｄｅｃｒｉｐｔｉｏｎ　Ｆａｉｌｕｒｅが起きているかどうかをチェックすることができる。

【００８３】なお、コンテンツ配信サーバ１３は、専用のハードウェア装置としてデザインすることも可能であるが、ワークステーション（ＷＳ）又はパーソナル・コンピュータ（ＰＣ）と呼ばれる一般的な計算機システム上で所定のサーバ・アプリケーションを起動させるという形態で実現することも可能である。

【００８４】また、図４には、コンテンツ配信サーバ１３からコンテンツの配信サービスを受ける携帯情報端末１５の機能構成を模式的に示している。同図に示すように、携帯情報端末１５は、携帯電話１４経由でネットワークに接続してコンテンツ配信サーバ１３との間でメッセージの送受信を行うための送受信部５１と、コンテンツ配信サーバ１３などの外部装置から受信した電子署名を検証する電子署名検証部５２と、乱数生成部５３と、携帯情報端末１５自身の電子署名を生成する電子署名生成部５４と、送信メッセージの暗号化や受信メッセージの復号化を行う暗号処理部３５と、発生した乱数や携帯情報端末１５自身の秘密鍵・公開鍵や通信相手の公開鍵など所定のデータを保存するメモリ部５６と、認証処理部５７と、コンテンツ配信サーバ１３から受信したコンテンツを再生利用するコンテンツ再生部５８と、コンテンツ配信サーバ１３からの課金要求を処理する課金処理部５９を備えている。

【００８５】電子署名検証部５２は、送受信部５１で受信されたコンテンツ配信サーバ１３の電子署名ＣｅｒｔｉｆｏｃａｔｉｏｎＢを検証するとともに、この電子署名に含まれるコンテンツ配信サーバ１３の公開鍵E_bを取り出して、メモリ部５６に保存しておく。

【００８６】乱数発生部５３は、相互認証に用いられる乱数N_aを生成したり、セッション・キーの種となる乱数S_aを生成する。これらの乱数N_a及びS_aは、コンテンツ配信サーバ１３などの通信相手とセッションが確立している間はメモリ部５６に保存されている。

【００８７】電子署名生成部５４は、携帯情報端末１５自身の公開鍵E_aをメモリ部５６から取り出して、このF_aを含んだ電子署名ＣｅｒｔｉｆｉｃａｔｉｏｎＡを生成して、送受信部５１からコンテンツ配信元となるコンテンツ配信サーバ１３に送信する。

【００８８】暗号処理部５５は、コンテンツ配信サーバ１３などの通信相手に送信するデータを相手の公開鍵E_bで暗号化したり、逆にコンテンツ配信サーバ１３から受信したデータを自分自分の秘密鍵で復号化したりする。また、暗号処理部５５は、通信相手と交換し合った互いのセッション・キーの種を基にセッション・キーを生成して、認証処理後の送信データの暗号化に用いるこ

とができる。

【００８９】認証処理部５７は、コンテンツ配信サーバ１３などのコンテンツ配信元との間で認証処理を行う。例えば、通信相手からの受信メッセージに含まれるデータのハッシュ値を計算して、同じく受信メッセージに含まれるハッシュ値と照合することにより、通信相手が本物であるか否かを判別することができる。また、相互認証処理にＮＴＲＵ公開鍵暗号方式を用いているが、認証処理部５７は、ハッシュ値の照合により、Ｄｅｃｒｉｐｔｉｏｎ　Ｆａｉｌｕｒｅが起きているかどうかをチェックすることができる。

【００９０】図５には、携帯情報端末１５とコンテンツ配信サーバ１３間で行われる相互認証の処理手順の一例を示している。但し、携帯情報端末１５は、ＮＴＲＵ公開鍵暗号方式による公開鍵E_aとこれに非対称な秘密鍵を持ち、同様に、コンテンツ配信サーバ１３は、ＮＴＲＵ公開鍵暗号方式による公開鍵F_bとこれに非対称な秘密鍵を持つものとする。

【００９１】まず、クライアントとしての携帯情報端末１５は、自分の公開鍵E_aを含んだ電子署名ＣｅｒｔｉｆｉｃａｔｉｏｎＡを送信する（Ｐ１）。

【００９２】コンテンツ配信サーバ１３側では、この電子署名ＣｅｒｔｉｆｉｃａｔｉｏｎＡを受信すると、電子署名検証部３２でこれを検証する。

【００９３】電子署名が正しいと判断された場合には、乱数発生部３３で、相互認証に用いる乱数N_bと、セッション・キーの種となる乱数S_bを発生させる。さらに、適当なハッシュ・アルゴリズムにより、セッション・キーの種S_bのハッシュ値Ｈａｓｈ（S_b）を計算する。そして、N_b、S_b、Ｈａｓｈ（S_b）を携帯情報端末１５の公開鍵E_aで暗号化して、これを電子署名生成部３４で生成した電子署名ＣｅｒｔｉｆｉｃａｔｉｏｎＢとともに携帯情報端末１５に送信する（Ｐ２）。

【００９４】携帯情報端末１５側では、電子署名ＣｅｒｔｉｆｉｃａｔｉｏｎＢと暗号データE_a（Nb，Sb，Ｈａｓｈ（S_b））からなるメッセージを受信すると、相互認証とＤｅｃｒｉｐｔｉｏｎ　Ｆａｉｌｕｒｅの検証を行う。

【００９５】図６には、携帯情報端末１５側で行われる相互認証とＤｅｃｒｉｐｔｉｏｎＦａｉｌｕｒｅの検証を合わせて行うための処理手順をフローチャートの形式で示している。以下、このフローチャートに従って説明する。

【００９６】まず、電子署名検証部５２で電子署名ＣｅｒｔｉｆｉｃａｔｉｏｎＢを検証する（ステップＳ１１）。

【００９７】電子署名が正しいと判断された場合には（ステップＳ１２）、暗号化処理部５５において、暗号化データE_a（N_b，S_b，Ｈａｓｈ（S_b））を復号化して、N_b、S_b、Ｈａｓｈ（S_b）を取り出す（ステップＳ１３）。

【００９８】次いで、復号化されたセッション・キーの種S_bに対して同じハッシュ・アルゴリズムを適用してそのハッシュ値Ｈａｓｈ'（S_b）を作成し（ステップＳ１４）、これが受信データから取り出されたハッシュ値Ｈａｓｈ（S_b）と一致するか否かを判別する（ステップＳ１５）。ハッシュ値が等しくなることによって、携帯情報端末１５側ではＤｅｃｒｉｐｔｉｏｎ　Ｆａｉｌｕｒｅが発生していないことを確認することができる。

【００９９】再び図５に戻って説明する。Ｄｅｃｒｉｐｔｉｏｎ　Ｆａｉｌｕｒｅがないことが確認された後、携帯情報端末１５では、乱数発生部５３で、相互認証に用いる乱数N_aと、セッション・キーの種となる乱数S_aを発生させる。さらに、適当なハッシュ・アルゴリズムにより、セッション・キーの種S_aのハッシュ値Ｈａｓｈ（S_a）を計算する。そして、Na、Sa、Ｈａｓｈ（Sa）を携帯情報端末１５の公開鍵F_bで暗号化して、これを、相互認証用の乱数N_bとともにコンテンツ配信サーバ１３に送信する（Ｐ３）。

【０１００】コンテンツ配信サーバ１３側では、乱数Ｎｂと暗号データＥｂ（Ｎａ，Ｓａ，Ｈａｓｈ（S_a））からなるメッセージを受信すると、相互認証とＤｅｃｒｉｐｔｉｏｎ　Ｆａｉｌｕｒｅの検証を行う。

【０１０１】図７には、コンテンツ配信サーバ１３側で行われる相互認証とＤｅｃｒｉｐｔｉｏｎ　Ｆａｉｌｕｒｅの検証を合わせて行うための処理手順をフローチャートの形式で示している。以下、このフローチャートに従って説明する。

【０１０２】まず、認証処理部３７で、受信メッセージに含まれるN_bが、乱数生成部３３で生成した乱数N_bと等しいか否かを判別して（ステップＳ２１）、通信相手が暗号化メッセージE_a（N_b，S_b，Ｈａｓｈ（S_b））からN_bを取り出せたか否か、すなわち本物かどうかを確認する。

【０１０３】乱数N_bが一致すると判断された場合には、暗号化処理部５５において、暗号化データE_b（N_a，S_a，Ｈａｓｈ（S_a））を復号化して、N_a、S_a、Ｈａｓｈ（S_a）を取り出す（ステップＳ２２）。

【０１０４】次いで、復号化されたセッション・キーの種S_aに対して同じハッシュ・アルゴリズムを適用してそのハッシュ値Ｈａｓｈ'（S_a）を作成し（ステップＳ２３）、これが受信データから取り出されたハッシュ値Ｈａｓｈ（S_a）と一致するか否かを判別する（ステップＳ２４）。ハッシュ値が等しくなることによって、コンテンツ配信サーバ１３側ではＤｅｃｒｉｐｔｉｏｎ　Ｆａｉｌｕｒｅが発生していないことを確認することができる。

【０１０５】再び図５に戻って説明する。Ｄｅｃｒｉｐｔｉｏｎ　Ｆａｉｌｕｒｅがないことが確認された後、コンテンツ配信サーバ１３は、復号化された乱数N_aを

携帯情報端末１５に送り返す（Ｐ４）。

【０１０６】携帯情報端末１５側では、受信したNaが乱数生成部５３で生成したN_aと等しいか否かを判別して、通信相手が暗号化メッセージE_t（N_a，S_a，Ｈａｓｈ（S_a））からN_aを取り出せたか否か、すなわち本物かどうかを確認する。

【０１０７】そして、上述したような手続により、携帯情報端末１５及びコンテンツ配信サーバ１３が通信相手を相互認証するとともに、自分自身がＮＴＲＵ公開鍵暗号方式においてＤｅｃｒｉｐｔｉｏｎ　Ｆａｉｌｕｒｅを起していないことを確認し終えたならば、交換し合ったセッション・キーの種S_a及びS_bを併せてセッション・キーを作り出す。そして、誤命処理や、コンテンツ暗号鍵の送信などは、このセッション・キーを用いた安全な通信路上で行うことができる。

【０１０８】２つのセッション・キーの種S_a及びS_bを用いて、例えば以下の方法によりセッション・キーを生成することができる。

【０１０９】（１）S_a及びS_bのＸＯＲ（Exclusive OR：排他的論理和）値をセッション・キーとする。
（２）S_aの上位バイトとS_bの上位バイトを合わせたものをセッション・キーとする。

【０１１０】このような、各端末上で生成された種Sa及びSbからセッション・キーを生成することにより、お互いが正しく公開鍵で暗号化された乱数を復号化することができた場合（すなわち、ＤｅｃｒｉｐｔｉｏｎＦａｉｌｕｒｅがない場合）にのみ、セッション・キーを作り出すことができる。

【０１１１】そして、その後のデータのやり取りを、セッション・キーで暗号化して送受信することにより、第３者による改竄や盗聴を防ぐことができる。

【０１１２】図８には、携帯情報端末１５とコンテンツ配信サーバ１３間で行われる相互認証の処理手順に関する他の例を示している。但し、携帯情報端末１５は、ＮＴＲＵ公開鍵暗号方式による公開鍵E_aとこれに非対称な秘密鍵を持ち、同様に、コンテンツ配信サーバ１３は、ＮＴＲＵ公開鍵暗号方式による公開鍵E_bとこれに非対称な秘密鍵を持つものとする。

【０１１３】まず、クライアントとしての携帯情報端末１５は、自分の公開鍵E_aを含んだ電子署名ＣｅｒｔｉｆｉｃａｔｉｏｎＡを送信する（Ｐ１１）。

【０１１４】コンテンツ配信サーバ１３側では、この電子署名ＣｅｒｔｉｆｉｃａｔｉｏｎＡを受信すると、電子署名検証部３２でこれを検証する。

【０１１５】電子署名が正しいと判断された場合には、乱数発生部３３で相互認証に用いる乱数N_bを発生させ、これを携帯情報端末１５側の公開鍵E_aで暗号化して、これを電子署名生成部３４で生成した電子署名ＣｅｒｔｉｆｉｃａｔｉｏｎＢとともに携帯情報端末１５に送信する（Ｐ１２）。

【０１１６】携帯情報端末１５側では、電子署名ＣｅｒｔｉｆｉｃａｔｉｏｎＢと暗号データE_a（N_b）からなるメッセージを受信すると、電子署名検証部３２で電子署名ＣｅｒｔｉｆｉｃａｔｉｏｎＢの検証を行う。電子署名が正しいと判断された場合には、暗号化処理部５５において、暗号化データF_a（N_b）を復号化して、N_bを取り出して、そのハッシュ値Ｈａｓｈ（N_b）を作成する。さらに、乱数生成部５３で相互認証に用いる乱数N_aを発生させ、コンテンツ配信サーバ１３側の公開鍵E_bでこれを暗号化する。そして、このようにして作成されたE_b（N_a）及びＨａｓｈ（N_b）を含むメッセージを、コンテンツ配信サーバ１３に送信する（Ｐ１３）。

【０１１７】コンテンツ配信サーバ１３側では、E_b（N_a）及びＨａｓｈ（N_a）を含むメッセージを受信すると、携帯情報端末１５についての認証処理を行う。図９には、コンテンツ配信サーバ１３側で行う携帯情報端末１５についての認証手続をフローチャートの形式で示している。以下、このフローチャートに従って、携帯情報端末１５についての認証手続について説明する。

【０１１８】まず、所定のハッシュ・アルゴリズムにより乱数発生部３２で発生した乱数N_bのハッシュ値を計算する（ステップＳ３１）。そして、計算されたハッシュ値が、携帯情報端末１５から受信したハッシュ値Ｈａｓｈ（N_b）と等しいか否かを判別する（ステップＳ３２）。

【０１１９】これらハッシュ値が等しい場合、携帯情報端末１５が正しくメッセージを復号化できたことを確認できるので、携帯情報端末１５が本物の通信相手であることが判る。

【０１２０】次いで、受信した暗号化データE_t（N_a）を暗号処理部３５で復号化して、携帯情報端末１５側の乱数N_aを取り出す（ステップＳ３３）。

【０１２１】そして、所定のハッシュ・アルゴリズムによりこの乱数N_aのハッシュ値Ｈａｓｈ（N_a）を計算して（ステップＳ３４）、これを携帯情報端末１５に送信する（ステップＳ３５）（Ｐ１４）。

【０１２２】また、コンテンツ配信サーバ１３は、乱数発生部３３で発生させた乱数N_bと、携帯情報端末１５からの受信データを復号化して得られた乱数N_aを基に、セッション・キーを生成する（ステップＳ３６）。

【０１２３】携帯情報端末１５側では、ハッシュ値Ｈａｓｈ（N_b）を含むメッセージを受信すると、コンテンツ配信サーバ１３についての認証処理を行う。図１０には、携帯情報端末１５側で行うコンテンツ配信サーバ１３についての認証手続をフローチャートの形式で示している。以下、このフローチャートに従って、コンテンツ配信サーバ１３についての認証手続について説明する。

【０１２４】まず、所定のハッシュ・アルゴリズムにより乱数発生部５２で発生した乱数N_aのハッシュ値を計

算する（ステップＳ４１）。そして、計算されたハッシュ値が、コンテンツ配信サーバ１３から受信したハッシュ値Ｈａｓｈ（Ｎｂ）と等しいか否かを判別する（ステップＳ４２）。

【０１２５】これらハッシュ値が等しい場合、コンテンツ配信サーバ１３が正しくメッセージを復号化できたことを確認できるので、コンテンツ配信サーバ１３が本物の通信相手であることが判る。

【０１２６】次いで、携帯情報端末１５は、乱数発生部５３で発生させた乱数Ｎａと、コンテンツ配信サーバ１３からの受信データを復号化して得られた乱数Ｎｂを基に、セッション・キーを生成する（ステップＳ４３）。

【０１２７】図８からも判るように、上述した相互認証プロトコルによれば、コンテンツ配信サーバ１３と携帯情報端末１５間の通信路上では、セッション・キーの種となるＮａ及びＮｂなる乱数は、ハッシュがかけられた状態又は暗号化された状態でのみ現れる。したがって、仮に認証段階で通信路を傍受されたとしても、セッション・キーを推測されることは不可能である。また、コンテンツ配信サーバ１３と携帯情報端末１５は、一方から送られてきたハッシュ値と自分で作り出したハッシュ値が等しいことから、相手が正常に復号化できたことを確認することができる。

【０１２８】２つのセッション・キーの種Ｎａ及びＮｂを用いて、例えば以下の方法によりセッション・キーを生成することができる。

【０１２９】（１）Ｎａ及びＮｂのＸＯＲ（Exclusive OR：排他的論理和）値をセッション・キーとする。

（２）Ｎａの上位バイトとＮｂの上位バイトを合わせたものをセッション・キーとする。

（３）ＮａとＮｂの和のハッシュ値Ｈａｓｈ（Ｎａ＋Ｎｂ）をセッション・キーとする。

【０１３０】このような、各端末上で生成された種Ｎａ及びＮｂからセッション・キーを生成することにより、お互いが正しく公開鍵で暗号化された乱数を復号化することができた場合にのみ、セッション・キーを作り出すことができる。

【０１３１】［追補］以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、本明細書の記載内容を限定的に解釈するべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１３２】

【発明の効果】以上詳記したように、本発明によれば、音楽や画像などの有料コンテンツの配信において課金処理時に相互認証を好適に行うことができる、優れた相互認証システム及び相互認証方法、相互認証装置、並びに記憶媒体を提供することができる。

【０１３３】また、本発明によれば、公開鍵暗号方式を用いて機器間の相互認証を好適に行うことができる、優れた相互認証システム及び相互認証方法、相互認証装置、並びに記憶媒体を提供することができる。

【０１３４】また、本発明によれば、比較的処理が軽い公開鍵暗号方式を用いて携帯端末のような組み込み機器のような資源が限られた機器環境でも相互認証を行うことができる、優れた相互認証システム及び相互認証方法、相互認証装置、並びに記憶媒体を提供することができる。

【０１３５】本発明によれば、ＮＴＲＵ公開鍵暗号方式を用いたプロトコルによりサーバとクライアント間の相互認証を行うことができる。また、このプロトコルで送受信されるセッション・キー用の乱数を基にセッション・キーを作り出して、認証後のデータ送受信を暗号化して行うことができる。また、ＮＴＲＵの公開鍵暗号方式は、復号化時に元のデータとは異なるＤｅｃｒｉｐｔｉｏｎ　Ｆａｉｌｕｒｅがあることが知られているが、送信データ中にセッション・キーの種となる乱数とそのハッシュ値を加えることにより、Ｄｅｃｒｉｐｔｉｏｎ　Ｆａｉｌｕｒｅが起きているかどうかをチェックできるようにして、確かなセッション確立でセッション・キーを共有することができる。

【０１３６】したがって、本発明によれば、第３者によって見破られることがなく、安全にサーバとクライアント間の通信を行うことができる。例えば、Ｅ－Ｃｏｍｍｅｒｃｅなどにおける個人データ送信や、本人認証、課金システムなどに適用することができる。

【０１３７】従来のＳＳＬ（Secure Socket Layer）などの相互認証プロトコルは、処理が重いため端末には不向きである。これに対し、ＮＴＲＵの暗号化方式は処理が軽いことや簡単なプロトコルであることから、携帯電話や携帯情報端末などの組み込み型機器に実装することが可能である。

【図面の簡単な説明】

【図１】携帯端末に対してコンテンツ配信サービスを提供するネットワーク・システムの構成を模式的に示した図である。

【図２】本実施形態に係るネットワーク・システム上でのコンテンツ配信サービスの流れを概略的に示したフローチャートである。

【図３】コンテンツ配信サーバ１１の機能構成を模式的に示したブロック図である。

【図４】携帯情報端末１５の機能構成を模式的に示したブロック図である。

【図５】携帯情報端末１５とコンテンツ配信サーバ１３間で行われる相互認証の処理手順の一例を示したフロー図である。

【図６】携帯情報端末１５側で行われる相互認証とＤｅ

ｃｒｉｐｔｉｏｎ　Ｆａｉｌｕｒｅの検証を合わせて行うための処理手順を示したフローチャートである。

【図７】コンテンツ配信サーバ１３側で行われる相互認証とＤｅｃｒｉｐｔｉｏｎ　Ｆａｉｌｕｒｅの検証を合わせて行うための処理手順を示したフローチャートである。

【図８】携帯情報端末１５とコンテンツ配信サーバ１３間で行われる相互認証の処理手順に関する他の例を示したフロー図である。

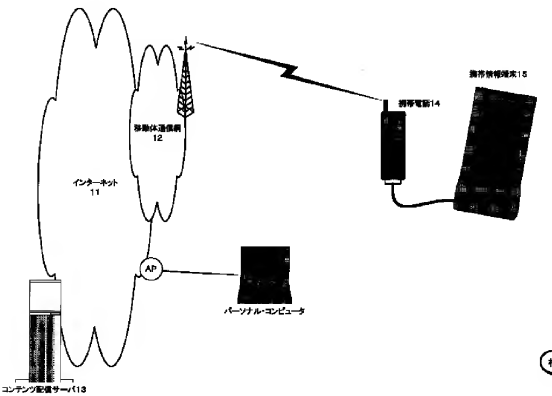
【図９】コンテンツ配信サーバ１３側で行う携帯情報端末１５についての認証手続を示したフローチャートである。

【図１０】携帯情報端末１５側で行うコンテンツ配信サーバ１３についての認証手続を示したフローチャートである。

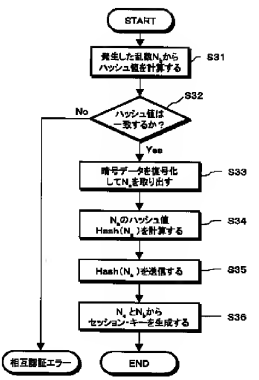
【符号の説明】

１１…インターネット
１２…移動体通信網
１３…コンテンツ配信サーバ
１４…携帯電話
＊１５…携帯情報端末
３１…送受信部
３２…電子署名検証部
３３…乱数生成部
３４…電子署名生成部
３５…暗号化処理部
３６…メモリ部
３７…認証処理部
３８…コンテンツ蓄積部
３９…課金処理部
５１…送受信部
５２…電子署名検証部
５３…乱数生成部
５４…電子署名生成部
５５…暗号化処理部
５６…メモリ部
５７…認証処理部
５８…コンテンツ再生部
５９…課金処理部

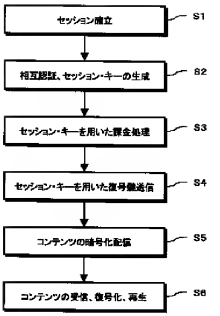
【図１】



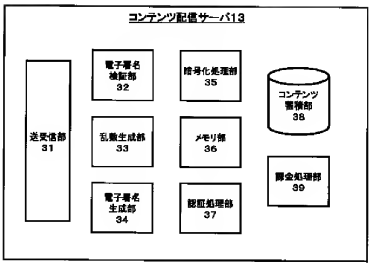
【図９】



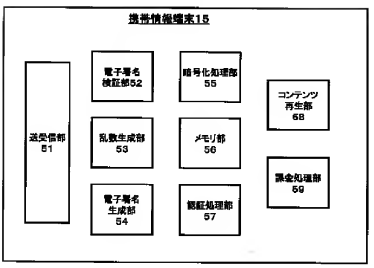
【図２】


セッション確立
S1
相互認証、セッション・キーの生成
S2
セッション・キーを用いた課金処理
S3
セッション・キーを用いた復号鍵送信
S4
コンテンツの暗号化配信
S5
コンテンツの受信、復号化、再生
S6

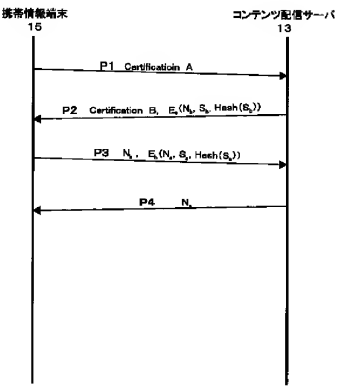
【図３】


コンテンツ配信サーバ13
送受信部
31
電子署名
検証部
32
暗号化処理部
35
コンテンツ
管理部
38
乱数生成部
33
メモリ部
36
課金処理部
39
電子署名
生成部
34
認証処理部
37

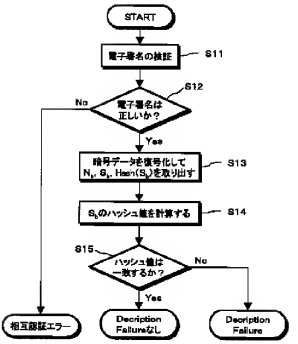
【図４】


携帯情報端末15
送受信部
51
電子署名
検証部52
暗号化処理部
55
コンテンツ
再生部
58
乱数生成部
53
メモリ部
56
課金処理部
59
電子署名
生成部
54
認証処理部
57

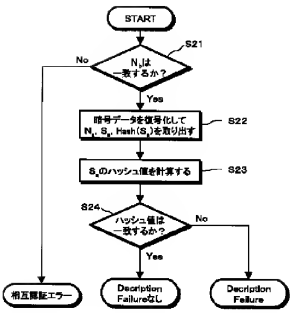
【図５】


携帯情報端末
15
コンテンツ配信サーバ
13
P1　Certificatoin A
P2　Certification B,　$E_A(N_A, S_B, Hash(S_B))$
P3　N_A,　$E_B(N_A, S_B, Hash(S_B))$
P4　N_A

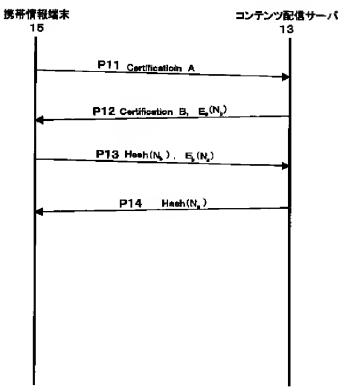
【図６】



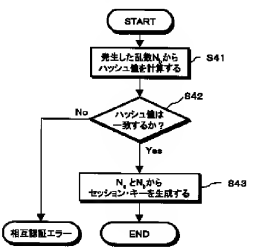
【図７】



【図８】



【図１０】



フロントページの続き

(51)Int.Cl.[7]	識別記号	F I	ﾃｰﾏｺｰﾄﾞ(参考)
G06F 17/60	ZEC	H04L 9/00	675B

Fターム(参考)　5B085 AE04 AE08
5J104 AA07 AA09 AA18 KA01 KA03
KA05 LA03 NA02 NA03 NA12
PA07 PA11